National Security Telecommunications and Information Systems Security Committee

NSTISSP No. 12
January 2001

NATIONAL INFORMATION ASSURANCE (IA) POLICY FOR U.S. SPACE SYSTEMS

National Security Telecommunications and Information Systems Security Committee

CHAIR

1. (U) Presidential Decision Directive (PDD) No. 49, Subject: National Space Policy, dated 19 September 1996, has established that U.S. space activities are critical to the national security of the United States. Commercial space activities are also closely linked to the operation of the U.S. Government's critical infrastructures as identified in Presidential Decision Directive (PDD) No. 63, Subject: Critical Infrastructure Protection, dated 22 May 1998, and may, on occasion, be leveraged to satisfy national security requirements. Based on the importance of these activities, it is imperative that a comprehensive, national-level information assurance (IA) space policy be developed, promulgated, and adopted that will ensure the confidentiality, authenticity, integrity, availability, and survivability of associated communications and communications networks under a wide range of peace or war time cyber threat scenarios.

2. (U) The primary objective of this policy is to ensure that IA is factored into the planning, design, launch, sustained operation, and deactivation of all U.S. space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems. The policy also serves to remind users of space assets outside the national security community that they may also wish to factor IA into those space activities associated with the operation and/or maintenance of critical U.S. infrastructures.

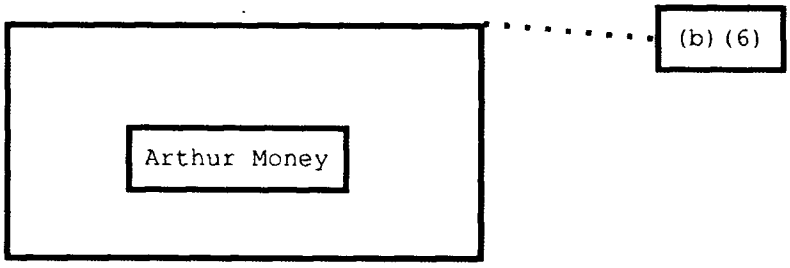
3. (U) Effective with its date of signature, this policy supersedes National Telecommunications and Information Systems Security Policy (NTISSP) No. 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems (U), dated 17 June 1985, and National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 100, National Policy on Application of Communications Security to Command Destruct Systems, dated 14 September 1999.

NSTISSC Secretariat [redacted], National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716

(b) (3)-P.L. 86-36 [redacted]

4. (U) The issuance of this policy is reflective of the Committee's desire to remain responsive to the changing information systems security needs of the nation. It is consistent with the future directions for the Committee documented in NSTISSC-034-99, Subject: Information Assurance Position Paper, dated 26 April 1999.

5. (U) NSTISSC Representatives may obtain additional copies of this policy from the address listed on the first page of the FOREWORD. U.S. Government contractors should contact their appropriate government Contracting Office Representative (COR) regarding further distribution and dissemination of this document.



(U) NATIONAL INFORMATION ASSURANCE (IA) POLICY FOR U.S. SPACE SYSTEMS

SECTION I - (U) SCOPE

1. (U) This policy is applicable to all U.S. Government or commercially owned and operated space systems (i.e., U.S. space systems) used to collect, generate, process, store, display, or transmit/receive national security information; all supporting or related national security systems; and to all U.S. Government Departments and Agencies involved in the acquisition, launch, operation, maintenance, or lease of these same systems.

SECTION II - (U) POLICY

2. (U) U.S. space systems (i.e., those space systems launched, owned, and operated by the U.S. Government or operated for the benefit of the U.S. Government); as well as those launched, owned, and operated by commercial entities (either domestic or foreign/international), used to collect, generate, process, store, display, or transmit/receive national security information, or information related to the operation of critical U.S. infrastructures are critical to the defense of the nation and are important components of its critical infrastructures.

3. (U) The successful launch and operation of these systems must be based on the application and integration of a combination of information assurance (IA) products, services, measures, and techniques providing acceptable or desired levels of assurance for associated information systems and networks and the information they collect, generate, process, store, display, or transmit/receive. These IA products, services, measures, and techniques must address or accommodate the following requirements in a balanced manner:

a. (U) Confidentiality, i.e., assuring that information is not disclosed to unauthorized persons, processes, or devices.

b. (U) Authentication, i.e., establishing the validity of a transmission, message, or originator, or as a means of verifying an individual's authorization to receive specific categories of information.

c. (U) Data Integrity, i.e., ensuring that data is unchanged from its sources and has not been accidentally or maliciously modified, altered, or destroyed.

d. (U) Availability, i.e., ensuring timely and reliable (on demand) access to data and information services for authorized users.

e. (U) Non-repudiation, i.e., assuring the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

f. (U) Personnel security and the physical security of communications security (COMSEC) and IA products and their associated keying material.

4. (U) Designers, developers, planners, and end users of U.S. space systems shall ensure that IA requirements are considered and addressed during the entire life-

cycle of all U.S. space systems used to collect, generate, process, store, display, or transmit national security information, as well as all supporting or related national security systems. "Life-cycle" includes all stages of planning, design, research and development, test and evaluation, deployment, operations, product improvement, and system retirement.

5. (U//~~FOUO~~) Based on threat analysis and risk assessments, data owners, platform owners, launch operators, and mission operators shall identify their IA requirements and acquire and implement those products, services, measures, or techniques (e.g., anti-jamming, anti-spoofing, etc.) necessary for providing the desired or required levels of assurance.

6. (U) The following IA requirements shall be addressed and satisfied for U.S. space systems used to collect, generate, process, store, display, or transmit national security information:

a. (U) Approved U.S. cryptographies shall be used to provide confidentiality for:

1) (U) The command/control up-links.
2) (U) The data links used to transmit national security information between the ground and space platforms.
3) (U) The cross-links between space platforms; and
4) (U) The downlinks from space platforms to mission ground or processing centers.

b. (U) Supporting or related national security systems will be similarly protected.

c. (U) A Secure Command Destruct System (SCDS) shall be required for all launch vehicles used to place in orbit space platforms which are used to collect, generate, process, store, display, or transmit national security information. This policy requirement applies to both U.S. Government and U.S. commercial launch vehicles, which may be used to launch U.S. space platforms.

(NOTE: (U) U.S. Government Departments and Agencies may also wish to consider the application of SCDS technologies to other launch applications (e.g., testing and/or research and development of sub-orbital vehicles or unmanned aircraft) where there are concerns for public safety, or the integrity of the platform may be placed at risk as a result of unintentional, unauthorized, or other interfering signals.)

7. (U//~~FOUO~~) A Cryptographic Security Plan (CSP) shall be required for the launch of all space systems incorporating approved U.S. cryptographies. The CSP will be subject to prior review and approval by the National Security Agency (NSA). At a minimum, the CSP shall:

a. (U) Describe the safeguards (e.g., transportation, storage, and integration procedures) that will be afforded to approved U.S. cryptographies and associated keying materials that are supportive of the development, launch, and/or operation of the space system.

b. (U//~~FOUO~~) Require the immediate reporting (to the NSA) of the loss or suspected loss of any approved U.S. cryptographies and associated keying materials and, in the event of launch failures, include reasonable plans for recovering these materials and returning them to U.S. control.

8. (U) Approved U.S. cryptographies shall be required for use on commercial imagery satellites where there is either foreknowledge or a reasonable expectation (based on documented U.S. planning or strategies), that such platforms may, during periods of international crises or wartime hostilities, be used to satisfy national security requirements involving classified information, or information determined to be critical or essential to the operational or organizational missions of U.S. Government entities.

9. (U//~~FOUO~~) The release to or provision of any approved U.S. cryptographies (manifested in either hardware, software, firmware, or associated keys) to foreign nations or international space consortia shall be subject to review and approval of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) in accordance with the requirements of National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 8.

10. (U) Subject to policy and guidance for non-national security information and systems, U.S. Government Departments and Agencies may wish to consider the IA requirements of this policy for those space systems which collect, generate, process, store, display, or transmit information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems which may be associated with the operation and/or maintenance of critical infrastructures. This would include confidentiality requirements for all associated data links.

11. (U) Definitions associated with this policy are contained in ANNEX A. For purposes of clarity, the policy requirements of this document are summarized in matrix form in ANNEX B.

SECTION III - (U) RESPONSIBILITIES

12. (U) The Director, National Security Agency (DIRNSA) shall:

a. (U) Review and approve all cryptographies intended to satisfy IA requirements for confidentiality and authenticity associated with this policy.

b. (U) Provide IA advice and assistance to U.S. Government Departments and Agencies prior to their contracting for the design, development, manufacture, acquisition, launch, and operation of any space system requiring the use of approved U.S. cryptographies.

c. (U) Review and approve all CSPs prior to the launch of U.S. or foreign space systems incorporating approved U.S. cryptographies.

d. (U) Establish and maintain a database of all U.S. and foreign space systems which employ approved U.S. cryptographies, and a list of which approved U.S. cryptographies each employs.

13. (U) Heads of U.S. Government Departments and Agencies shall:

a. (U) Ensure compliance with the IA requirements of this policy for the acquisition, launch, operation, and maintenance of all U.S. space systems which are used to collect, generate, transmit, process, store, or display national security information, as well as for any related national security systems. Compliance includes:

1) (U) Programming those funds required to acquire those products, services, measures or techniques necessary to provide acceptable or desired levels of IA; and

2) (U) Ensuring that IA products, services, and measures are integrated, activated, and sustained as critical security components of all U.S. space systems.

b. (U) Ensure, through licensing or contractual relationships, that the requirements of this policy are imposed on those U.S. or foreign commercial entities involved in the launch, operation, or maintenance of U.S. space systems.

c. (U) Determine whether this policy should be applied to those space systems under their control, purview, or cognizance that may be directly related to the operation and maintenance of critical U.S. infrastructures.

SECTION IV – (U) QUALIFICATIONS, EXCLUSIONS, AND EXCEPTIONS

14. (U) This policy establishes minimum requirements for providing IA for U.S. space systems used to collect, generate, transmit, process, store, or display national security information, or for related systems that utilize approved U.S. cryptographies. Depending on threats and risk management deliberations and decisions, heads of U.S. Government Departments and Agencies may impose more stringent requirements on the operation of their systems.

15. (U) Aircraft, operational ballistic missile weapons systems, munitions, and sub-orbital test vehicles are specifically excluded from the requirements of this policy.

16. (U) The SCDS requirements of this policy do not apply to the commercial launch of commercial satellites that do not use approved U.S. cryptographies nor are ever intended to provide support to, or be part of a national security system.

17. (U//~~FOUO~~) Exceptions to this policy may be granted by the NSTISSC on a case-by-case basis. Requests for exceptions, including a justification and explanatory details, shall be forwarded through the Director, National Security Agency (DIRNSA), ATTN: [redacted] who shall provide appropriate recommendations for NSTISSC consideration. Where time constraints or operational considerations may not allow for the full review and approval of the NSTISSC membership, the Chairman of the NSTISSC is hereby authorized to approve waivers to this policy which may be necessary to support sensitive U.S. space activities.

18. (U//~~FOUO~~) Nothing in this policy should be interpreted as altering or superseding the existing authorities of the Director of Central Intelligence.

(b)(3)-P.L. 86-36

ANNEX A – DEFINITIONS

1. (U) *Approved U.S. Cryptographies*: Hardware, firmware, or software implementations of algorithms which have been reviewed and approved by the National Security Agency (NSA), the purposes of which are to provide authentication or confidentiality for national security information or systems.

2. (U) *Command Up-Link*: Data transmission path established for purposes of positioning or relocating space platforms (i.e., orbital insertions or adjustments), or for effecting tasking changes to the mission payload(s).

3. (U) *Communications Security (COMSEC)*: Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (NSTISSI No. 4009)

4. (U) *Critical Infrastructures*: Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

5. (U) *Flight Termination System (FTS)*: A capability designed and incorporated into launch vehicles which provides for the deliberate termination of the launch process that has been determined to be anomalous, and which might pose a threat to lives or property if the launch is not terminated.

6. (U) *Information Assurance (IA)*: Information operations (IO) intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

7. (U) *Information Systems Security (INFOSEC)*: Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those necessary to detect, document, and counter such threats. (NSTISSI No. 4009)

8. (U) *Launch Vehicle*: The rocket or self-powered portion of the flight component of a space system that is being tested (i.e., research, development, testing and engineering (RDT&E) activities) or otherwise used in an operational context to propel itself or a space platform and its associated mission payload out of the earth's atmosphere.

9. (U) *National Security Information*: Information that has been determined, pursuant to Executive Order 12958, dated 17 April 1995, or any predecessor order, to be classified and to require protection against unauthorized disclosure.

10. (U) *National Security Systems*: Telecommunications or information systems operated by the U.S. Government (or on behalf of the U.S. Government) the function, operation or use of which:

Involves intelligence activities;
Involves cryptologic activities related to national security;
Involves command and control of military forces;
Involves equipment that is an integral part of a weapon or weapons system; or

Is critical to the direct fulfillment of military or intelligence missions (but does not include a system that is to be used for routine administrative applications including payroll, finance, logistics, and personnel management applications). (Title 40 USC Section 1452)

11. (U) *Protection*: The application, integration, and certification of products or services in a communications system or network for purposes of providing a desired level of confidence that transmitted information and associated systems and networks will be available on demand and free from malicious disruption or exploitation. The objective of protection is to satisfactorily achieve some or all of the components of Information Assurance.

12. (U) *Secure Command Destruct System (SCDS)*: The cryptographic component of the FTS. An approved U.S. cryptography incorporated into the launch operations center and launch vehicle which provides a capability for the secure or authenticated transmissions of a flight termination command or the activation of the FTS.

13. (U) *Space Platform*: An orbiting satellite, spacecraft, or space station developed, launched, and operated for purposes of providing specified products or services to users or customers.

14. (U) *Space System*: Those components necessary for the effective launch and operation of a space platform. They include the telecommunications, data links, and information systems associated with launch control facilities, the launch vehicle, the space platform and its associated payload, command and control and mission down/cross link communications, and mission ground and/or processing stations.

15. (U) *U.S. Space Systems*: Those space systems launched, owned, and operated by the U.S. Government (or operated for the benefit of the U.S. Government), as well as those launched, owned and operated by commercial entities (either domestic or foreign/international), that are used to collect, generate, process, store, display, or transmit/receive national security information, or information related to the operation of critical U.S. infrastructures.

ANNEX B - INFORMATION ASSURANCE/SECURITY REQUIREMENTS								
SPACE ACTIVITIES	"Life-cycle" IA Planning	Flight Termination System	Secure Command Destruct	Secure Command Uplink	Secure Platform Crosslinks	Secure Payload Downlinks	Secure Ground-to Ground Communications	Cryptographic Security Plan (CSP)
National Security Payload:								
- U.S. Government Launch	YES	YES	YES	YES	YES	YES	YES	YES
- U.S. Commercial Launch	YES	YES	YES	YES	YES	YES	YES	YES
- Foreign Commercial Launch[1]	Optional	Optional	Optional	YES	YES	YES	Optional	YES
- Int'l Consortia Launch[1]	Optional	Optional	Optional	YES	YES	YES	Optional	YES
Non-National Security Payload:								
- U.S. Government Launch	Optional	Optional	Optional	Optional	Optional	Optional	Optional	NO[2]
- U.S. Commercial Launch	Optional	Optional	NO	Optional	Optional	Optional	Optional	NO[2]
- Foreign Commercial Launch	Optional	Optional	NO	Optional	Optional	Optional	Optional	NO[2]
- Intl Consortia Launch	Optional	Optional	NO	Optional	Optional	Optional	Optional	NO[2]
Critical Infrastructure Related:	Optional	Optional	NO	Optional	Optional	Optional	Optional	NO[2]
Mission Critical Or Mission Essential:	Optional	Optional	Optional	Optional	Optional	Optional	Optional	NO[2]

Explanation of Terms:

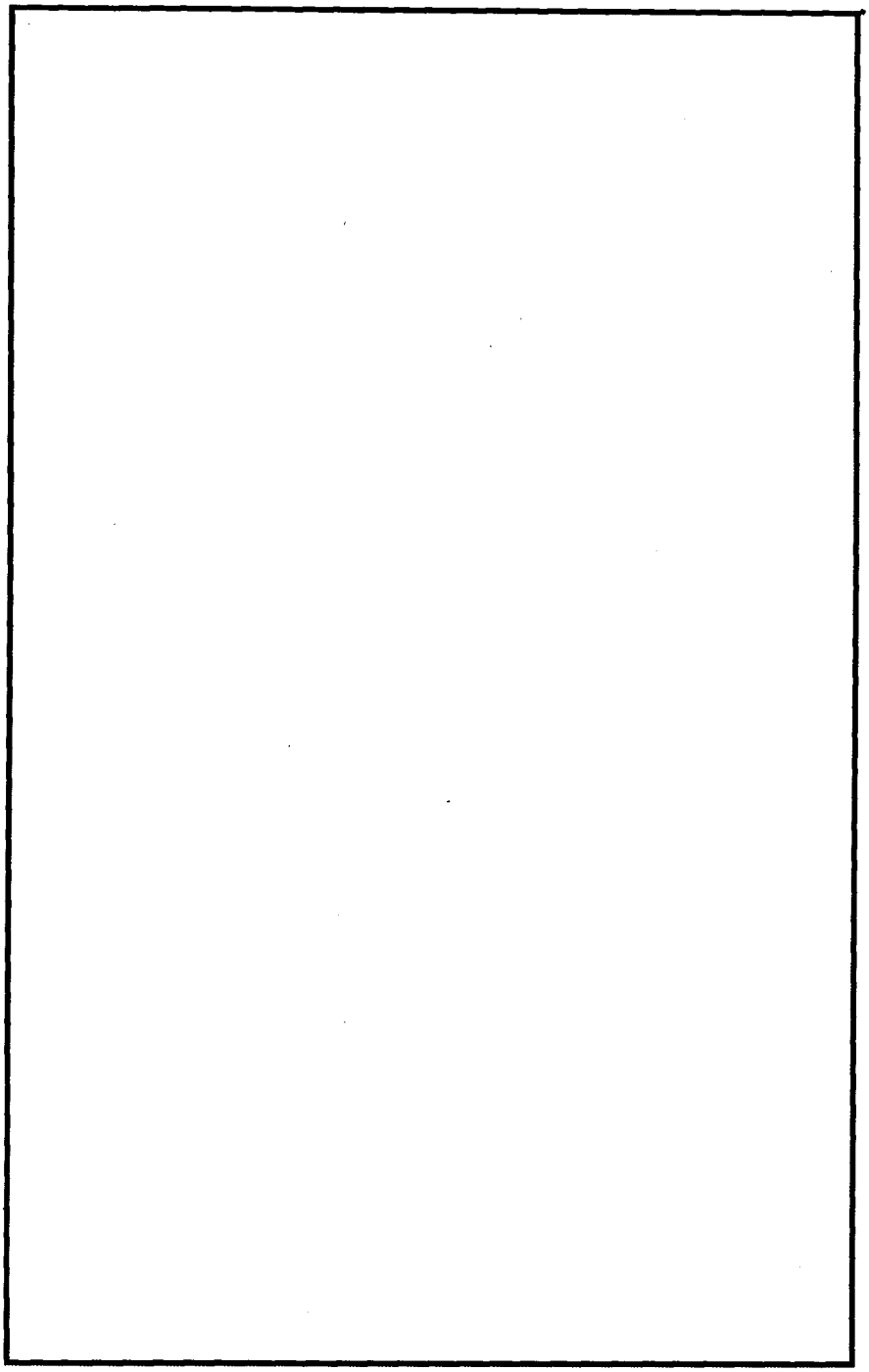
YES: A specific requirement of this policy.
NO: Not a requirement of this policy.
OPTIONAL: A discretionary decision based on risk management decisions to include inputs from the end user, launch operators, and range commanders. Not a firm requirement, but implementation provides increased assurances for the safety, security, and integrity of space launch and operational activities.

Footnote:

[1] *Addresses situations where there is foreknowledge that launch payloads (e.g., commercial imaging satellites) may, during periods of international crises or wartime hostilities, be used to satisfy national security requirements.*
[2] *This NO becomes a YES if Approved U.S. Cryptographies are involved.*

(b)(3)-P.L. 86-36

DISTRIBUTION:



(b)(3)-P.L. 86-36